Statement of C. Paul Robinson, Director
Sandia National Laboratories

United States House of Representatives
Committee on Commerce
Subcommittee on Oversight and Investigations

July 11, 2000

Statement of C. Paul Robinson, Director
Sandia National Laboratories

United States House of Representatives
Committee on Commerce
Subcommittee on Oversight and Investigations
July 11, 2000

SUMMARY

The Secretary of Energy and the directors of the nuclear weapon laboratories share the same desire for effective security. Both are stymied by bureaucratic inefficiency. The National Nuclear Security Administration (NNSA) is our last best hope for fixing our security problems in a systematic way. The new administrator of the NNSA will not succeed unless he has full authority and free rein to redesign the structure of the nuclear complex from the ground up.

An erroneous perception has arisen that the laboratories have a culture of indifference or even contempt for security. Sandia National Laboratories' culture was shaped by its heritage of industrial management. Our industrial roots gave us a strong cultural commitment to security.

Sandia implemented an Integrated Safeguards and Security Management System, which is designed to integrate responsibility for security into the daily work of every employee. Employees and contractors who handle classified matter are required and trained to protect it from unauthorized access. Significant overall improvements in the cyber-security of the nuclear weapons complex have been accomplished at substantial cost in 1999 and 2000. However, formidable challenges to computer security still confront the NNSA and other federal agencies.

In the early 1990s, DOE required the laboratories to discontinue formal document accountability for Secret Restricted Data. The laboratory directors were never comfortable with that change. Sandia National Laboratories will re-implement formal document accountability for Secret Restricted Data in the near future. Similarly, in the middle 1990s, DOE's classification program was changed in a way that weakened its effectiveness.

Clearly, the NNSA laboratories need to continue their focus on enhancing security. However, security enhancements must be implemented in a way that creates robust security within user-friendly work environments.

INTRODUCTION

Mr. Chairman and distinguished members of the committee, thank you for the opportunity to testify today. I am Paul Robinson, director of Sandia National Laboratories. Sandia National Laboratories is managed and operated for the U.S. Department of Energy by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation.

Sandia National Laboratories is a multiprogram laboratory of the National Nuclear Security Administration (NNSA). We share responsibility for the design and stewardship of nuclear weapons with Los Alamos and Lawrence Livermore National Laboratories. Sandia's job is the design, development, and certification of nearly all of the non-nuclear subsystems of nuclear weapons. Our responsibilities include arming, fuzing, and firing systems; safety, security, and use-control systems; engineering support for production and dismantlement of nuclear weapons; and surveillance and support of weapons in stockpile. We perform substantial work in programs closely related to nuclear weapons, such as nuclear intelligence, nonproliferation, and treaty verification technologies. As a multiprogram national laboratory, Sandia also performs research and development for DOE's energy offices, as well as work for other agencies when our unique capabilities can make significant contributions.

SECURITY AND BUREAUCRACY

I appreciate your invitation to make a statement today addressing the topic, "Weaknesses in Classified Information Security Controls at DOE's Nuclear Weapon Laboratories." Secretary Richardson said in testimony before the Senate Armed Services Committee on June 21 that he has done more to improve security during his two years in office than had been accomplished in the previous twenty years by his predecessors. I have been active in the DOE/AEC community for all my career, and I can vouch for his claim. Yet, for all the well-motivated actions and strong leadership that has been so evident, I cannot say that our important restricted data and national security information are more secure than ever before. My hesitancy derives from a surfeit of complications that surround security.

The Secretary and the laboratory directors share the same desire for effective security performance; we are not at odds. But I believe we are both stymied by the bureaucratic sclerosis of the agency. From below, the laboratories are frustrated with a maze of conflicting rules and directives from various offices of the Department, together with team after team of inspectors that descend upon us. From above, the Secretary has resorted to managing the security problems by issuing directives from his own office, rather than relying on the agency's internal mechanisms to generate and implement reforms. This game of catch-up between the top of the agency and those who must

implement the directives, with far too little communication on the chances for success or the unforeseen consequences of new policies, has been a problem in almost all areas of support for DOE missions—in environment, safety, and health issues, in business practices, and in security.

The President's Foreign Intelligence Advisory Board (PFIAB) appreciated the magnitude of this problem. Their report, "Science at Its Best; Security at Its Worst," issued last year, referred to DOE as a "big, byzantine, and bewildering bureaucracy." In regard to security performance, the PFIAB found that "multiple chains of command and standards of performance negated accountability, resulting in pervasive inefficiency, confusion, and mistrust" (page I). It concluded that "real and lasting security and counterintelligence reform at the weapons labs is simply unworkable within DOE's current structure and culture" (page 46). The PFIAB's recommendations, of course, were the impetus for the legislation creating the semi-autonomous National Nuclear Security Administration within the Department of Energy.

It is my belief that the circumstances in DOE are not the fault of any individuals, certainly not the people who are in charge or occupy key positions in the Department of Energy today. As the President's Foreign Intelligence Advisory Board found, the single most identifiable factor that led to the current state of affairs was the relentless growth of bureaucracy. My definition of bureaucracy is when well-meaning, capable people find it difficult to accomplish their mission responsibilities because of multiple lines of authority and bureaucratic hurdles that must be overcome.

I believe the National Nuclear Security Administration is our last best hope for fixing our security problems in a systematic way. By "fixing" I mean creating a security culture across the complex (federal workers and contractors) that achieves teamwork and mutual commitment to the goals of security. As things stand now, there is little sense of collaborative work toward a shared goal in security. Security in DOE is a "house divided"—those who make the rules, and those who must follow them. There is little discussion with the field by those who write guidance and policy. The people who really know the technologies that can be helpful have little input. It is, as has been said before, a "dysfunctional" relationship.

The new administrator of the NNSA, General John A. Gordon, has quite a challenge before him. But as qualified and as competent as he is, he will not succeed unless he has full authority and free rein to redesign the structure of the nuclear complex from the ground up. I know that the laboratory directors and the federal managers of the NNSA will fully support him in this undertaking.

SANDIA HAS A POSITIVE SECURITY CULTURE

An erroneous perception has arisen that the laboratories have a culture of indifference or even contempt for security. I can tell you that this perception is grossly inaccurate for Sandia National Laboratories, and I believe it is inaccurate for the other NNSA laboratories as well. Certainly we have had challenges and problems in various aspects of security performance, but I take issue with the belief that we have an ingrained or widespread "attitude problem" toward security at Sandia.

Sandia's laboratory culture was shaped by its industrial heritage, which began in 1949 under the management of AT&T Bell Laboratories and continued after 1993 with Lockheed Martin Corporation. Our industrial roots gave us a strong cultural commitment to security. Industrial laboratories are very conscious of the need to keep proprietary information secure. As I enumerated in previous testimony to this committee, Sandia has a long history of originating and implementing innovations that have improved security without direction from DOE (see Questions for the Record for my testimony to this subcommittee on October 26, 1999). And we also have a history—as I will illustrate later in my statement—of challenging policy changes mandated from above that would weaken our protections and controls on classified materials.

In June 1999, the Secretary of Energy called for a stand-down of operations at the Defense Programs laboratories to conduct an intensive two-day session of security training. Contrary to reports that laboratory staff were resistant to this training, our staff participated with great interest and with a positive attitude. We had 93 percent staff participation during the stand-down, and we achieved the full 100 percent shortly thereafter. (The seven percent difference consisted of people on previously scheduled vacations or essential business travel, illness absences, and critical job functions such as security and medical staffing.) The thoughtful dialog and suggestions offered by employees during the security sessions clearly demonstrated a laboratory culture of positive concern and advocacy for effective security.

I was not at all surprised that the inspectors from the DOE Office of Independent Oversight and Performance Assurance remarked on the positive and cooperative attitude among Sandia managers with whom they worked during the 1999 inspection of Sandia National Laboratories. I frequently get similar comments from other audit and inspection teams. Sandia has a culture of respect for security, and people notice it. At the close-out meeting of the most recent visit of the DOE Oversight and Performance Assurance Team in June, it was encouraging to receive informal verbal feedback from the inspectors to the effect that Sandia is currently meeting all requirements and is above and beyond minimal requirements in many areas. The team commented that they found it refreshing to see a sense of ownership for security at the manager level. They also remarked that

Sandia's custodians of classified matter are well-versed in their responsibilities; they know what to do and are doing it well.

SECURITY MANAGEMENT AT SANDIA

Sandia has implemented an Integrated Safeguards and Security Management System (ISSMS) for all its security responsibilities. As the name implies, the goal of Integrated Safeguards and Security Management is to incorporate responsibility for security into the daily work of every employee. We can't just bring in security experts and give them the job of inspecting-out the defects; every single person bears responsibility to build-in and maintain sound security measures. This is a necessary attribute of a stable security culture.

ISSMS establishes clear and unambiguous lines of authority and responsibility for ensuring that secure operations are established and maintained at all organizational levels. Authority and responsibility for security at Sandia National Laboratories begins with me and flows via my deputy laboratory director to the line vice presidents that report to her. Sandia's Chief Security Officer coordinates the enabling resources that support the line executives in their security responsibilities. ISSMS ensures that personnel possess the training, knowledge, and abilities necessary to discharge their security responsibilities. It also provides a way to allocate resources efficiently to address security and operational needs.

Our ISSMS methodology stresses the need to identify applicable security standards and requirements before work is performed. Administrative and engineering controls to prevent and mitigate security risks are tailored to the work being performed and are designed into work processes. While we make use of a "fresh-set-of-eyes" in examining security practices and draw on the knowledge and experience of security professionals, we gain the involvement and creativity of those actually carrying out the work in developing security procedures that make sense in the workplace.

SANDIA'S PARTICIPATION WITH THE NNSA'S NUCLEAR EMERGENCY SEARCH TEAM (NEST)

The National Nuclear Security Administration plays a vitally important support role in combating acts of nuclear terrorism through its Nuclear Emergency Search Team (NEST). NEST provides the FBI with technical assistance in response to terrorist use or threat of use of a nuclear or radiological device in the United States. NEST also supports the State Department in a similar role overseas. Another team, the Accident Response Group (ARG), has the different mission of

providing technical support in response to accidents involving U.S. nuclear weapons while they are either in the custody of DOE or the military services.

The highly selective force that makes up the cadre of deployment personnel for NEST and ARG are mostly from the nuclear weapons laboratories. To be on the NEST team, an individual must be approved by both line and program management, have certain essential technical skills, pass a physical examination, and take additional training. My experience is that NEST members are conscientious and dedicated individuals with a high sense of duty. NEST personnel volunteer for a mission which, if not successful, could have severe consequences for the nation and be fatal for the team.

Sandia National Laboratories contributes a number of team members to the NEST. Sandia does not possess any NEST computer media similar to that reported as missing by the Los Alamos group. Sandia's role in NEST is different from that of Los Alamos and Lawrence Livermore, focusing largely on the non-nuclear electronic subsystems of warheads and bombs as well as methods for calculating the consequences of dispersal events and methods for containment.

Sandia does maintain some classified computer media and lap-tops under the ARG program. This information is significantly different from the NEST media at Los Alamos. This classified material has all been accounted for. Furthermore, within the last three weeks, we instituted stricter controls for these items, including a two-person rule and formal sign-in/sign-out procedures.

CLASSIFIED MATERIAL PROTECTION AND CONTROL

Sandia employees and contractors who handle classified matter are required to protect and control classified material from unauthorized, casual, and deliberate access. This requirement is one of the first things a new-hire is briefed on when he or she joins Sandia National Laboratories, and we continue to educate our personnel on the procedures that implement this policy throughout their careers through annual refresher training courses.

The core principles that we teach our employees regarding access to classified material are contained in Sandia's Safeguards and Security Guide, which is readily available as a reference on our internal network. Access to classified matter requires a job-related need-to-know, as determined by an individual's manager, as well as a proper security clearance.

As you know, Secretary Richardson distributed a memorandum on June 19, 2000, directing the implementation of certain enhanced protection measures at the NNSA laboratories. I welcome the emphasis on accountability that the memorandum so clearly communicates. Sandia took immediate steps to implement or commence work on the enhancement measures that are the

responsibility of the laboratories, and we will cooperate with the NNSA offices responsible for implementing other measures in their purview.

Controls for Vault Access

Sandia has explicit rules governing the storage of classified matter. Briefly, classified material must be stored in vaults or vault-type rooms (or in a military-style igloo similar to a vault-type room), or in key- or combination-lock containers approved by the General Services Administration and located in a locked and alarmed building. Sandia National Laboratories manages 166 vaults or vault-type rooms that store classified matter (documents or material)—114 at our New Mexico location and 52 at our California site.

In compliance with Secretary Richardson's memorandum of June 19, 2000 (received late on June 20), Sandia modified operating procedures for all vault access on June 21. We modified our log sheets to record the entrance and exit of all personnel. We also required that access/egress points for vaults be under continuous, positive control by personnel authorized for access to that specific vault. Or, for vault-type rooms (large vaults in which a number of people work) we required that the vault be occupied and that access by authorized personnel be controlled by an electronic system. In the absence of these controls, the vault must be in a locked and alarmed state.

Controls over Electronic Media

On June 15, 2000, Sandia's chief information officer initiated a lab-wide survey of removable classified electronic storage media. The objective of this survey was to determine that removable media are accounted for (to the extent possible in the absence of formal document accountability) and are properly stored. The survey found that all holdings were accounted for, except for two relatively minor issues which were immediately communicated to DOE via the Department's incident reporting system. The first issue involved a set of unclassified commercial software program disks that were treated as classified. The inquiry is still active, but has concluded that those disks contained no classified information. The other issue (reported on June 30) involves a single 3 1/2-inch, 1.44-megabyte diskette that has not yet been located. An inquiry is currently underway in accordance with DOE procedures.

Significant overall improvements in the cyber-security of the nuclear weapons complex have been accomplished at substantial cost in 1999 and 2000. However, many potential vulnerabilities continue to present formidable challenges to computer security. There are no easy solutions. Although encrypted removable media or media-less computing may have their places in a defensive system (and I believe they do), there are many ways for a sophisticated adversary to extract information in today's modern electronic environment. Removable media, email, hot mail, ftp file

transfer, http file transfer, port-enabled file transfers, laptops, modems, network sniffers, video-monitor-to-VCR converters, faxes, mail, copiers, two-way pagers, telephones, cell-phones, and computer trash are all potentially exploitable. Cyber-security is certainly the most formidable security challenge facing DOE and the federal government as a whole.

Because of the magnitude of the cyber-security challenge, a systems approach across the entire NNSA complex is required. I am very pleased that emergency supplemental funding for cyber-security upgrades has been approved by Congress as part of the FY2001 Military Construction Appropriations Bill. The funding is badly needed to combat cyber threats and vulnerabilities in a coordinated fashion throughout the nuclear weapons complex.

WEAKNESSES IN THE DOCUMENT ACCOUNTABILITY PROGRAM

Prior to 1991, DOE practiced full document accountability for all Secret data under its control. Document accountability was a formal system for inventorying and recording access to classified documents over the lifetime of the document, from creation to destruction. The system was analogous to—although much more rigorous than—the common library check-out system that was aptly cited by a member of this committee.

In February 1991, DOE modified its accountability rules to drop the requirement for formal document accountability over Secret National Security Information and "non-weapon Secret Restricted Data." (Restricted Data is a category of protected information created by the Atomic Energy Act that includes "data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power.")

In May 1992, DOE extended its Modified Accountability Program to include weapon-related Secret Restricted Data. DOE notified the laboratories that accountability requirements were being modified for all categories of Secret data for organizations that had met certain requirements, including having completed a 100 percent inventory and reconciliation of controlled documents in accordance with DOE Order 5635.1A.

The Modified Accountability Program was instituted by DOE to accommodate the National Industrial Security Program, which was intended to standardize security requirements among all federal agencies. It should be noted that prior to the Modified Accountability Program, DOE protected Secret Restricted Data with the same level of protection employed by the Department of Defense for Top Secret.

The modified accountability program eliminated the requirements for unique document numbers and maintenance of accountability records for documents, inventories, destruction

certificates, written authorizations to reproduce, and some internal receipting. Other security procedures not explicitly changed by the modified accountability program were unaffected.

Unfortunately, with the change in accountability, DOE lost the ability to track who was accessing which secret documents, a feature that had been a useful tool for counterintelligence analysis. While this change clearly saved money and made sense in the broader context of consistency across all federal agencies, it reduced our ability to quickly detect the absence of a document, and it eliminated our capability to formally monitor the access to secret classified matter. This statement applies to documents and information in printed form as well as to electronic media.

The laboratory directors were never comfortable with the change to Modified Document Accountability. At Sandia, we originally told DOE that we intended not to implement the Modified Accountability Program. In response, DOE told us that costs for full accountability would no longer be reimbursable under the operating contract. Sandia complied with DOE's requirement, but we left open local options for higher levels of accountability.

In January 1998, DOE moved to eliminate full document accountability for Top Secret Restricted Data as well (and for other categories of Top Secret information). As part of this change, DOE eliminated the "Top Secret Control Officer" positions at the laboratories. I am proud to say that staff at Sandia had better sense and continued to protect Top Secret data with full document accountability—a decision that I have fully endorsed.

Sandia National Laboratories has consistently maintained full accountability for all Top Secret data under its control. And in fact, we have also maintained document accountability over selected sets of Secret data that we felt merited ongoing accountability. These examples demonstrate the culture of respect for security that exists at our laboratory. Rather than resisting efforts to improve security (as has been charged by some critics of the laboratories), the record shows that we are more likely to resist efforts to weaken it.

On March 1, 1999—following a conference call of the three nuclear weapon laboratory directors with Under Secretary Ernest Moniz on the topic of Secret and Top Secret accountability—I faxed a request on behalf of the directors to the Under Secretary in which we recommended that the former controls over document accountability be reinstated as quickly as possible. We requested that the Under Secretary and the Department's counterintelligence official evaluate the feasibility of promptly reinstating full document accountability. This request was submitted to the Department's security bureaucracy, and to our knowledge it has never emerged.

I have twice brought the modified accountability problem to the attention of Congress in testimony: in my statement to the Senate Committee on Energy and Natural Resources on May 5, 1999, and to this very subcommittee on October 26, 1999.

In my judgment, we can no longer afford to wait for official reinstatement of the full document accountability policy. The security and counterintelligence benefits afforded by formal accountability decisively outweigh the costs. Moreover, formal document accountability will help protect conscientious employees from the indignity of criminal suspicion similar to what some employees had to endure in the recent Los Alamos incident. Therefore, I have decided that Sandia National Laboratories will re-implement formal document accountability for Secret Restricted Data under its control at the earliest feasible date. I have directed Sandia's Chief Security Officer to develop an implementation plan for this change.

WEAKNESSES IN THE CLASSIFICATION PROGRAM

In parallel with the changes in document accountability introduced by the Department of Energy in the middle 1990s, changes were also made to DOE's classification program that, in my view, introduced systemic weaknesses.

A Fundamental Classification Policy Review was recommended by a Classification Policy Study in July 1992. Based on that recommendation, Secretary Hazel O'Leary committed DOE to review all classification policies and related technical guidance, and then to revise classification guidance to reflect changes in policy. DOE's Fundamental Classification Policy Review was initiated in March 1995, and was a major component of Secretary O'Leary's Openness Initiative.

In April 1995, the President issued Executive Order 12958, "Classified National Security Information." This directive modified some of the existing rules concerning classification, but it introduced significant new provisions requiring agencies to perform large-scale reviews of material for potential declassification. However, the order explicitly exempted Restricted Data (RD), which is governed by the classification provisions of the Atomic Energy Act.

Even though Executive Order 12958 excluded Atomic Energy Act Restricted Data, the directive dramatically influenced DOE's thinking toward classification and declassification of RD during its Fundamental Classification Policy Review. The review concluded in July 1996 with recommendations for regulatory changes that substantially applied the provisions of Executive Order 12958 to Atomic Energy Act Restricted Data. The new regulations (10CFR1045) required large-scale periodic and systematic reviews of RD documents for declassification "based on the degree of public and researcher interest and likelihood of declassification upon review."

The declassification regulations, while well-intentioned, required a level of effort by the Department that it was not equipped to handle. As a result, the primary emphasis and deployment of manpower in the classification organization at DOE changed from effective administration of

classification responsibilities to effective management of the declassification efforts. The organization even changed its name from "Office of Classification" to "Office of Declassification."

It should be noted that some federal agencies used the process of "bulk declassification" as a mechanism to meet the requirements of Executive Order 12958. This practice often resulted in inappropriate information being released into the public domain without document-by-document review. The negative impact of these actions is still being felt today throughout the federal government.

It has become evident in the last few years that DOE's classification program is in crisis. As a profession, the classification field has become needlessly complex and arcane. The federal government's classification rules evolved over several decades and from different agencies, and they are rife with inconsistencies and legalistic complexities. The system is poorly indexed and coordinated. DOE classification officers rely on a body of some eight hundred sources of classification guidance for DOE source material alone; and they must be familiar with hundreds of other sources that govern the classification of National Security Information from other agencies. Classification professionals in the DOE community—and they are all technical-degreed personnel—often must use their subjective good judgment to resolve conflicting or unclear guidance.

To their credit, the DOE Office of Declassification embarked on a "Guidance Flattening Initiative" two years ago which should go a long way toward simplifying classification guidance and reducing conflicts. It would also be helpful if the classification community could define subsets of need-to-know categories to help us in administering the need-to-know principle. However, the classification community in DOE is disproportionately assigned to the management of the declassification effort, with a need to devote more effort to the efficient and effective management of the classification program.

IMPACT OF SECURITY ON THE WORK ENVIRONMENT

As a laboratory director, I am responsible for maintaining in top condition the infrastructure and human talent of one of the nation's foremost laboratories supporting vitally important national security objectives. I am worried about our pool of human talent to carry out this mission. Clearly, the NNSA laboratories need to continue their focus on enhancing security. But if security enhancements are implemented in a way that creates an atmosphere of mistrust, or generates unnecessary procedural burdens, or is perceived to be discriminatory against some groups, or dictates prescriptions that technical people have no input to, then the talent pool at the laboratories will begin to suffer.

Even without the security issues that the laboratories face today, we would still be having a tough time attracting and retaining talent in an economy that offers very attractive opportunities to technical graduates. Frankly, we are beginning to have a serious multidisciplinary staff retention issue. Poorly thought-out security and human reliability programs will only make that situation worse.

Rather, the NNSA must strive to create conditions that make security a natural way of doing one's job. We need user-friendly work environments that incorporate robust security features in a way that achieves maximum protection for secrets with minimal obstruction of productive activity. I am certain that the best solutions will be system solutions that begin by focusing on specific work activities and move outward from there to establish rules—as opposed to those that begin with rules, directives, and policies that originate at a great distance from the workplace. Robust and lasting security can only be achieved through the cooperative efforts of the laboratories, their M&O contractors, and NNSA management, with the firm but supportive oversight of Congress.

WITNESS DISCLOSURE FORM

Witness name: C. Paul Robinson

Capacity in which appearing: Representative

Name of entity being represented: Sandia National Laboratories

Curriculum vitae:

C. Paul Robinson serves as President of Sandia Corporation and Laboratory Director of Sandia National Laboratories. Sandia Corporation, a Lockheed Martin company, operates Sandia National Laboratories for the U.S. Department of Energy.

Dr. Robinson served as Vice President for Laboratory Development at Sandia from August 1991 through August 1995, having previously served as Director for Systems Analysis. During this period, he was responsible for strategic and operational planning, systems studies and analysis, information architectures, and new program initiatives.

From February 1988 to October 1990, Ambassador Robinson served as Chief Negotiator and Head of the U.S. delegation to the nuclear testing talks between the U.S. and the U.S.S.R. in Geneva, Switzerland. He was appointed by President Ronald Reagan, confirmed by the U.S. Senate, and subsequently reappointed by President George Bush. Those negotiations produced two major agreements: protocols to the Threshold Test Ban Treaty and the Peaceful Nuclear Explosions Treaty.

From December 1985 to February 1988, Dr. Robinson served as Senior Vice President and Principal Scientist of Ebasco Services, Inc., a major engineering and construction firm headquartered in New York. He was responsible for the advanced technology sector of the company, with major contracts in nuclear power, advanced power systems for defense and commercial energy needs, and support activities for major U.S. and international research projects.

Dr. Robinson spent most of his early career (1967-1985) at the Los Alamos National Laboratory, operated by the University of California for the U.S. Department of Energy. Initially he served as a physicist in the Nuclear Test Division, then became a member of the Advanced Concepts Group. He started the laboratory's efforts in laser spectroscopy, explosives-driven lasers, laser-induced chemistry, and isotope separation. Dr. Robinson led the laboratory's defense programs, with responsibility for nuclear weapons research, development, testing and stockpile maintenance, strategic defense initiatives, inertial fusion, nuclear materials and safeguards, advanced conventional weapons, as well as arms control and verification activities.

Dr. Robinson earned a Bachelor of Science degree in Physics from Christian Brothers College in 1963 and a Ph.D. in Physics from Florida State University in 1967. He also was awarded an honorary doctorate from Christian Brothers University in 1989.

He is presently a member of the Strategic Advisory Group for the Commander-in-Chief, U.S. Strategic Command, where he also serves as Chairman of the Policy Group, which is helping to develop new nuclear weapons policy for the post–Cold War period. In 1991, he served as chairman for the Presidential Technical Advisory Group on Verification of Warhead Dismantlement and Special Nuclear Materials Controls. He previously served on the Scientific Advisory Group on Effects for the Defense Nuclear Agency, as well as an advisor for other government agencies.

Federal funding of Sandia National Laboratories:

	Budget Authority in Millions			
	FY97	FY98	FY99	FY00 (est.)
DOE Operating Funding[1] (by primary secretarial office)				
Assistant Secretary for Defense Programs (DP)	$ 605	648	$ 680	$ 662
Assist. Secretary for Nonproliferation & National Security (NN)	122	133	134	145
Offices of Intelligence (IN) and Counterintelligence (CN)	5	5	6	6
Assistant Sec. for Environmental Management (EM)	91	94	72	69
Assistant Sec. for Energy Efficiency & Renewable Energy (EE)	43	43	53	46
Office of Science (SC)	33	34	34	36
Office of Nuclear Energy, Science and Technology (NE)	11	13	10	7
Assistant Secretary for Fossil Energy (FE)	7	7	6	6
Office of Fissile Materials Disposition (MD)	4	4	3	4
Other DOE offices	8	1	1	1
Sub-Total DOE Operating Funding	$ 929	981	$ 999	$ 982
Non-DOE Funding[2]				
Department of Defense	184	186	194	200
Nuclear Regulatory Commission	10	9	9	9
Orders or reconciling transfers from other DOE contractors	71	65	61	59
Other Federal Agencies (Other Than DoD/NRC)	46	47	34	32
Non Federal Entities Including CRADAs	46	57	58	54
Sub-Total Non-DOE Funding	$ 357	$ 364	$ 356	$ 354
Sandia Laboratories Operating	$1,286	$1,345	$1,355	$1,336
Sandia Laboratories Capital Equipment	28	25	35	32
Sandia Laboratories Construction	38	23	50	43
Sandia Laboratories Totals	$1,352	$1,393	$1,440	$1,411

Notes:

[1]Work for DOE is under a single prime contract.

[2]Number of contract actions for non-DOE sponsors:

Department of Defense	315	293	288	290
Nuclear Regulatory Commission	44	45	46	45
Orders or reconciling transfers from other DOE contractors	216	218	201	200
Other Federal Agencies (Other Than DoD/NRC)	95	84	105	100
Non Federal Entities Including CRADAs	214	251	288	275
Sub-Total Non-DOE Funded	884	891	928	910